US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

# Monthly Activity Summary
## - March 2010 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for March 2010. It includes current activity updates, technical and non-technical cyber security alerts, cyber security bulletins, and cyber security tips, in addition to other newsworthy events or highlights.

## Executive Summary

During March 2010, US-CERT issued 18 Current Activity entries, two (2) Technical Cyber Security Alerts, two (2) Cyber Security Alert, five (5) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month include updates released by Microsoft, Cisco, Apple, Oracle, CA, and Mozilla, along with malware activity related to the Zeus Trojan, the US Census, tax season, and copyright lawsuits.

## Contents



## Current Activity

Current Activity entries are high-impact security threats and vulnerabilities currently being reported to US-CERT. The table lists all of the entries posted this month, followed by a brief overview of the most significant entries.

| ***Current Activity for March 2010*** | |
|---|---|
| ***March 2*** | Microsoft Releases Security Advisory to Address VBScript Vulnerability |
| ***March 3*** | U.S. Census Bureau 2010 Census Campaign Warning |
| ***March 3*** | Microsoft Re-Releases Security Bulletin MS10-015 |
| ***March 4*** | Cisco Releases Multiple Security Advisories |
| ***March 4*** | Microsoft Releases Advance Notification for March Security Bulletin |
| ***March 8*** | Energizer DUO USB Battery Charger Software Allows Remote System Access |
| ***March 9*** | Microsoft Releases March Security Bulletin |

| *Current Activity for March 2010* | |
|---|---|
| ***March 12*** | Apple Releases Safari 4.0.5 |
| ***March 17*** | Zeus Trojan Campaign Warning |
| ***March 19*** | CA Releases Updates for ARCserve Backup |
| ***March 23*** | Mozilla Releases Firefox 3.6.2 |
| ***March 25*** | Cisco Releases Security Advisories for IOS Software |
| ***March 26*** | Copyright Infringement Lawsuit Email Scam |
| ***March 26*** | US Tax Season Phishing Scams and Malware Campaigns |
| ***March 29*** | Microsoft Releases Advance Notification for Out-of-Band Security Bulletin |
| ***March 29*** | Apple Releases Security Update 2010-002 and Mac OS X v10.6.3 |
| ***March 30*** | Microsoft Releases Out-of-Band Security Bulletin Update |
| ***March 31*** | Oracle Releases Critical Patch Update for Java SE and Java for Business |

- Microsoft issued updates for VBScript, Windows, Office, and Internet Explorer.
  - Microsoft Security Advisory 981169 addressed a vulnerability in VBScript. The vulnerability exists in the way that VBScript interacts with Windows Help files when using Internet Explorer. By convincing a user to view a specially crafted HTML document with Internet Explorer and to press the F1 key, an attacker could run arbitrary code with the privileges of the user running the application. Additional details are provided in a Microsoft Security Research & Defense blog entry and US-CERT Vulnerability Note VU#612021.
  - Microsoft re-released Microsoft Security Bulletin MS10-015 with an updated installation package that does not allow the security update to be installed on computers infected with malicious code. Microsoft also released a Fix-It Tool to determine if systems are compatible with the update. Additional details are provided in Microsoft Knowledge Base Article 977165, 980966, and the Microsoft Security Response Center (MSRC) Blog Post. Users who have already successfully installed the update for MS10-015 do not need to take any action.
  - The Microsoft Security Bulletin Summary for March 2010 addressed vulnerabilities in Windows and Office. These vulnerabilities may allow an attacker to execute arbitrary code.
  - The out-of-band bulletin MS10-018 addressed 10 vulnerabilities in Internet Explorer, including one previously announced in Microsoft Security Advisory 981374. The most severe of these vulnerabilities may allow an attacker to execute arbitrary code on the affected system.
- Cisco released multiple security advisories for a variety of applications.
  - Security advisory cisco-sa-20100303-cucm addressed multiple vulnerabilities in the Cisco Unified Communications Manager, which affect the Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP), and the Computer Telephony Integration (CTI) Manager services. Successful exploitation of these vulnerabilities could result in a denial-of-service condition and an interruption of voice services.
  - Security advisory cisco-sa-20100303-dmm addressed multiple vulnerabilities in the Cisco Digital Media Manager (DMM). Successful exploitation of these vulnerabilities could allow for information disclosure, unauthorized settings or system configuration changes, and disclosure of default credentials.

- Security advisory cisco-sa-20100303-dmp addressed a vulnerability in Cisco Digital Media Player. Successful exploitation of this vulnerability may allow an attacker to inject video or data content into a remote display.
- Cisco IOS Software Security Advisory bundled publication (cisco-sa-20100324-bundle) contains seven security advisories that addressed multiple vulnerabilities in Cisco IOS Software. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.

- Apple released updates to Safari and Mac OS X.
  - Safari 4.0.5 (HT4070) addressed multiple vulnerabilities in ColorSync, ImageIO, PubSub, Safari, and WebKit, which may allow a remote attacker to execute arbitrary code, cause a denial-of-service condition, obtain sensitive information, or bypass security restrictions.
  - Security Update 2010-002 and Mac OS X v10.6.3 (HT4077) addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code, obtain sensitive information, cause a denial-of-service condition, bypass security restrictions, or operate with elevated privileges.
- Oracle released a critical patch update to address 27 vulnerabilities in Java SE and Java for Business. These vulnerabilities are in the following components: ImageIO, Java 2D, Java Runtime Environment, Java Web Start, Pack200, Sound, JSSE, and HotSpot Server.
- CA released security notice CA20100318-01 to address vulnerabilities in the version of Java JRE bundled with ARCserve Backup. These vulnerabilities in Java JRE may allow an attacker to execute arbitrary code, bypass security restrictions, cause a denial-of-service condition, or obtain sensitive information.
- The Mozilla Foundation has released Firefox 3.6.2 to address multiple security issues, including a critical vulnerability that may allow a remote attacker to execute arbitrary code. Additional information regarding this vulnerability can be found in the US-CERT Vulnerability Note VU#964549 and Mozilla Foundation Security Advisory 2010-08.

## Technical Cyber Security Alerts

Technical Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits.

| *Technical Cyber Security Alerts for March 2010* | |
|---|---|
| ***March 9*** | TA10-068A Microsoft Updates for Multiple Vulnerabilities |
| ***March 30*** | TA10-089A Microsoft Internet Explorer Vulnerabilities |

## Cyber Security Alerts

Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits. They outline the steps and actions that non-technical home and corporate users can take to protect themselves.

| *Cyber Security Alerts (non-technical) for March 2010* | |
|---|---|
| ***March 9*** | SA10-068A Microsoft Updates for Multiple Vulnerabilities |
| ***March 30*** | SA10-089A Microsoft Internet Explorer Vulnerabilities |

## Cyber Security Bulletins

Cyber Security Bulletins are issued weekly and provide a summary of new vulnerabilities recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

| *Security Bulletins for March 2010* |
|---|
| SB10-060 Vulnerability Summary for the Week of February 22, 2010 |
| SB10-067 Vulnerability Summary for the Week of March 1, 2010 |
| SB10-074 Vulnerability Summary for the Week of March 8, 2010 |
| SB10-081 Vulnerability Summary for the Week of March 15, 2010 |
| SB10-088 Vulnerability Summary for the Week of March 22, 2010 |

A total of 513 vulnerabilities were recorded in the NVD during March 2010.

## Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users. The March tips focused on wireless networks and email clients. Links to the full versions of these documents are listed below.

| *Cyber Security Tips for March 2010* | |
|---|---|
| ***March 11*** | ST05-003 Securing Wireless Networks |
| ***March 31*** | ST04-023 Understanding Your Computer: Email Clients |

## Security Highlights

**Zeus Trojan Campaign Warning**
US-CERT received reports of malicious code circulated via spam email messages impersonating DHS. The attacks arrive via unsolicited email messages that may contain subject lines related to DHS or other government activity. These messages may contain a link or attachment. If users click on this link or open the attachment, they may be infected with malicious code, including the Zeus Trojan.

**United States (US) Tax Season Phishing Scams and Malware Campaigns**
US-CERT has received reports of an increased number of phishing scams and malware campaigns that take advantage of the US tax season. Due to the upcoming tax deadline, US-CERT reminds users to remain cautious when receiving unsolicited email that could be part of a potential phishing scam or malware campaign.

These phishing scams and malware campaigns may include the following: information that refers to a tax refund, warnings about unreported or under-reported income, offers to assist in filing for a refund, or details about fake e-file websites. These messages, which appear to be from the IRS, may

ask users to submit personal information via email or may instruct the user to follow a link to a website that requests personal information or contains malicious code.

Public reports indicated that tax season malware is actively circulating. This malware campaign may be using malicious code commonly known as Zeus or Zbot.

**Copyright Infringement Lawsuit Email Scam**
US-CERT is aware of public reports of an active email scam. These emails, which appear to come from seemingly legitimate law firms, indicate that someone has filed a copyright lawsuit against the message recipient. The messages may contain malicious attachments or web links. If a user opens the attachment or follows the link, malicious code may be installed on the user's system.

**US Census Bureau 2010 Census Campaign Warning**
US-CERT asks users to be vigilant during the US Census Bureau's 2010 Census campaign and to watch for potential census scams. According to the US Census 2010 website, they began delivery of the printed census forms to every resident in the United States on March 1, 2010. The only way to complete the census is by filling in the form using pen and ink; in some instances, census takers will be visiting households to complete the form face-to-face. It is important to understand that the US Census Bureau will not, under any circumstances, be providing an online option to complete the 2010 census form.

US-CERT encourages users and administrators to take the following measures to protect themselves from these types of phishing scams and malware campaigns:

- Do not follow unsolicited web links in email messages.
- Maintain up-to-date antivirus software.
- Review available information about the 2010 U.S. Census on the website.
- Familiarize yourself with what information the U.S. Census Bureau is collecting on the census form.
- Refer to Cyber Security Tip ST04-014 - Avoiding Social Engineering and Phishing Attacks.
- Refer to the IRS website related to phishing, email, and bogus website scams for scam samples and reporting information.

## *Contacting US-CERT*

If you would like to contact US-CERT to ask a question, submit an incident, or to learn more about cyber security, please use one of the methods listed below. If you would like to provide feedback on this report, or if you have comments or suggestions for future reports, please email info@us-cert.gov.

Web Site Address: http://www.us-cert.gov
Email Address: info@us-cert.gov
Phone Number: +1 (888) 282-0870
PGP Key ID: 0xCB0CBD6E
PGP Key Fingerprint: 2A10 30D4 3083 2D28 032F 6DE3 3D60 3D81 CB0C BD6E
PGP Key: https://www.us-cert.gov/pgp/info.asc